(12) UK Patent Application (19) GB (11) 2 186 404 (13) A

(43) Application published 12 Aug 1987

(21) Application No 8701956

(22) Date of filing 29 Jan 1987

(30) Priority data

(31) 826726 (32) 6 Feb 1986 (33) US
826725 6 Feb 1986

(51) INT CL[4]
G08B 29/00

(52) Domestic classification (Edition I)
G4H 13D 14A 14B 14G 1A 60 NK NNA
U1S 1270 2078 2188 2189 2192 2195 2196 G4H

(56) Documents cited
GB 1521273
EP A2 0117832
EP A2 0155773

(58) Field of search
G4H
Selected US specifications from IPC sub-class G08B

(71) Applicant
Notifier Company,

(Incorporated in USA-Connecticut),

3700 North 56th Street, Lincoln, Nebraska 68504, United States of America

(72) Inventors
Kevin T. Ruddell,
Stacy E. Gehman,
Brian D. Dawson

(74) Agent and/or Address for Service
J.W. Randall, Emhart Patents Department, PO Box 88, Ross Walk, Belgrave, Leicester LE4 5BX

(54) Security system with signal accuracy checking

(57) A security system having one or more sending units 10,11,12 for transmitting a digitised r-f signal representative of a condition such as fire, smoke, intrusion, battery condition, an emergency, or other condition to a central r-f receiving unit 18. The sending units 10,11,12 each include a microcomputer which shifts the data while adding the 6th bit without carry to bits one and three. After shifting is completed, the lower five bits remaining comprise a Cyclic Redundancy Code (CRC). The sending unit microcomputer generates a pseudo-random number, waits for a number of cycle periods equal to the pseudo-random number, then activates a transmitter 14,15,16 to send the data signal and the CRC to the receiving unit 18. The receiver 18 includes a microprocessor which recalculates the CRC and compares it with the received CRC, and those signals for which the codes are the same are gated to an output device to provide an indication of the conditions.

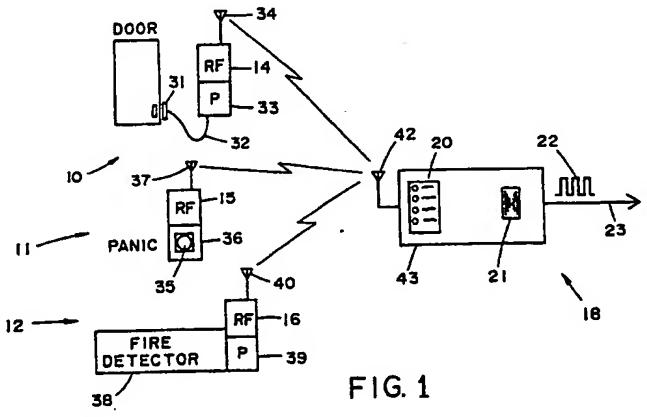

FIG. 1

GB 2 186 404 A

The specification as filed includes a computer program which is not here reproduced; it may be inspected in accordance with Section 118 of the Patents Act 1977.

2186404

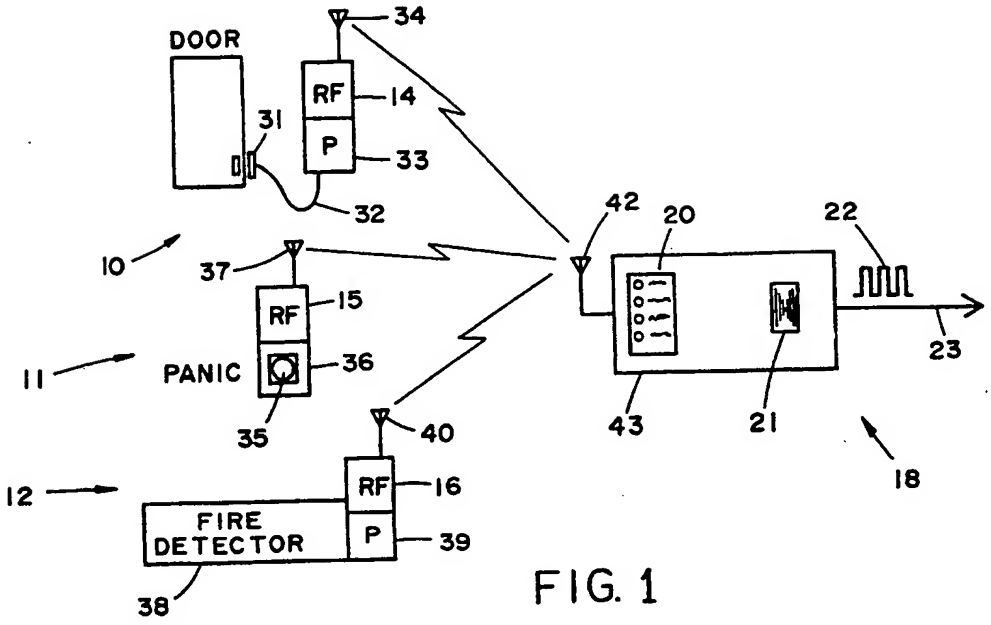

FIG. 1

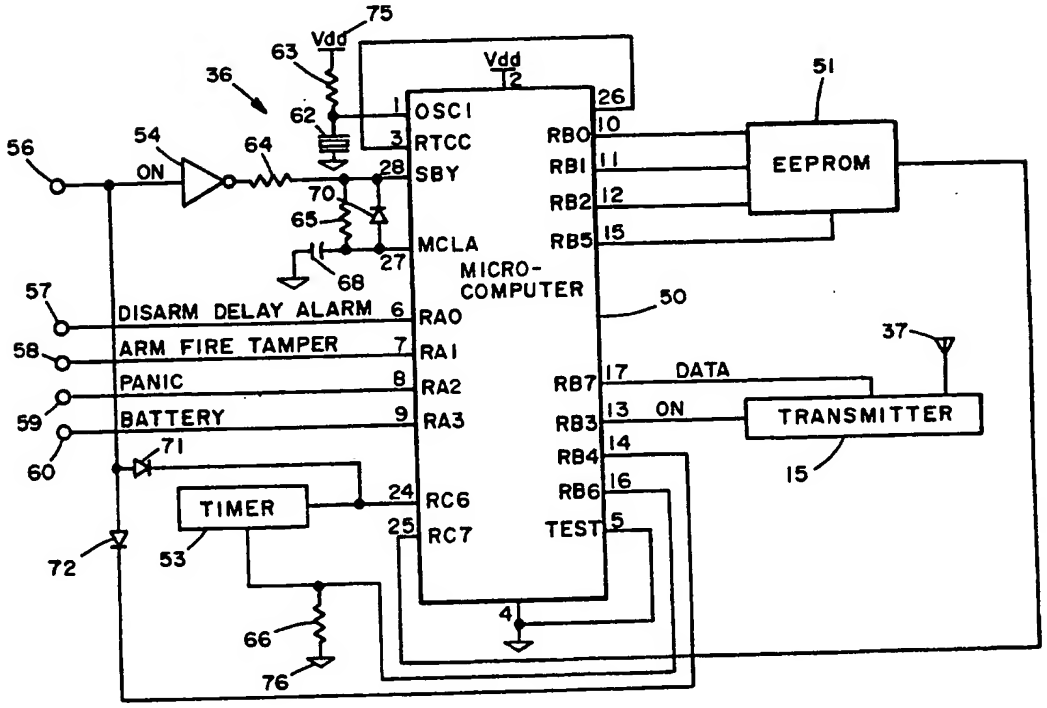

FIG. 2

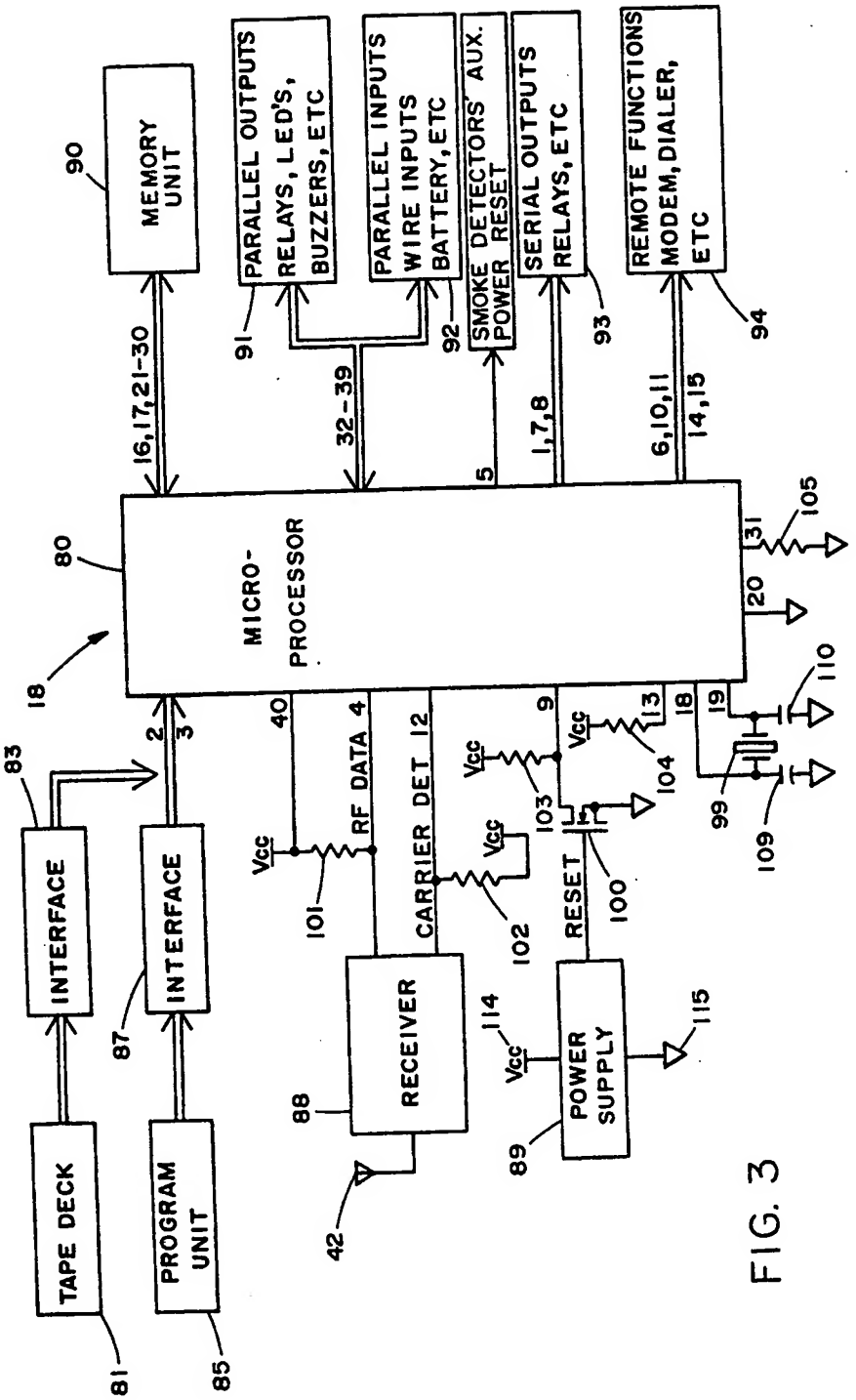
MEMORY UNIT
90
PARALLEL OUTPUTS RELAYS, LED'S, BUZZERS, ETC
91
PARALLEL INPUTS WIRE INPUTS BATTERY, ETC
92
SMOKE DETECTORS' AUX. POWER RESET
SERIAL OUTPUTS RELAYS, ETC
93
REMOTE FUNCTIONS MODEM, DIALER, ETC
94
16,17,21-30
32-39
5
1,7,8
6,10,11
14,15
MICRO-PROCESSOR
80
18
31
105
20
110
40
RF DATA 4
CARRIER DET 12
9
Vcc
13
104
18
19
103
101
102
RESET
100
99
109
2
3
83
INTERFACE
INTERFACE
87
RECEIVER
88
42
POWER SUPPLY
114
115
89
TAPE DECK
PROGRAM UNIT
81
85

FIG. 3

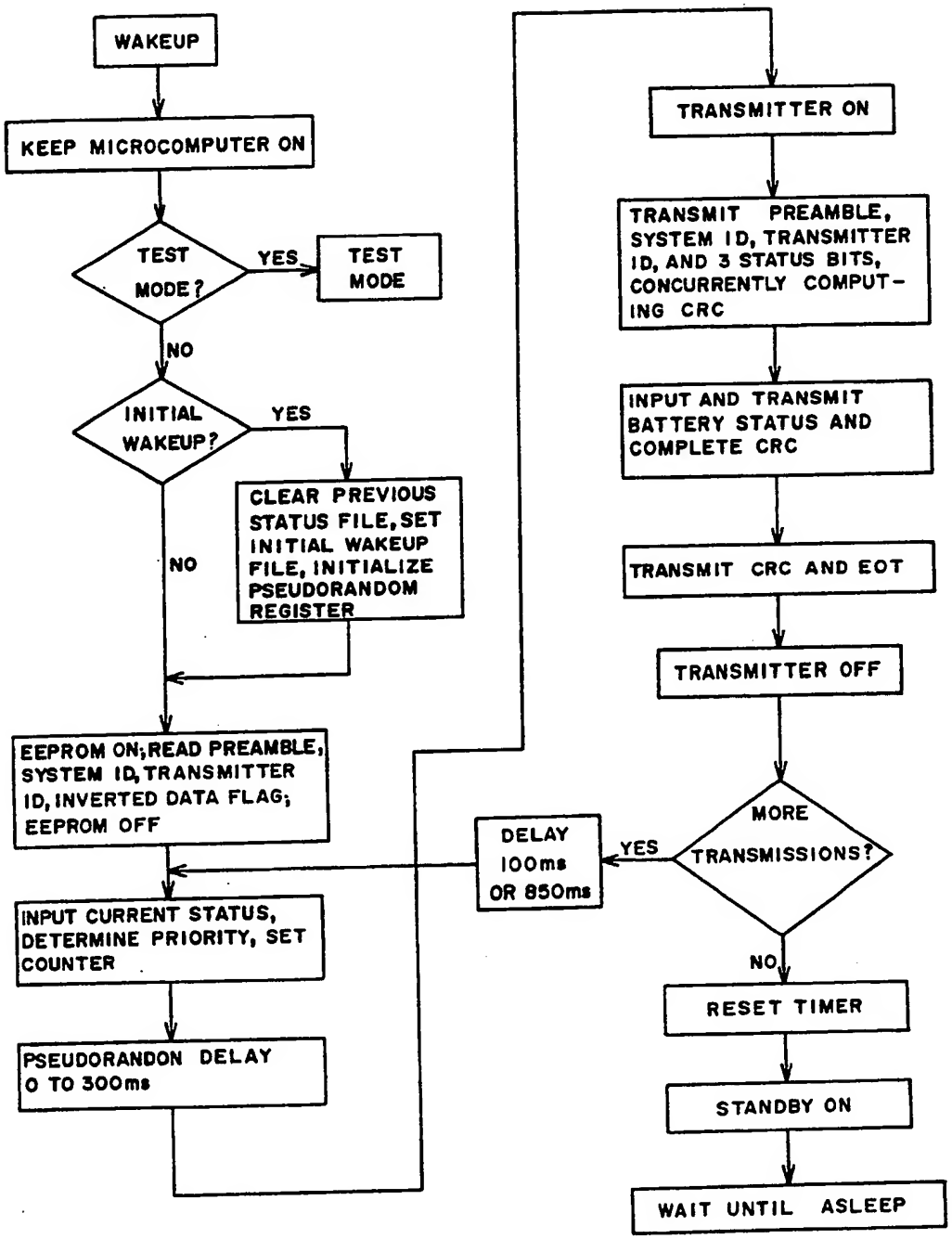
WAKEUP
KEEP MICROCOMPUTER ON
TEST MODE?
YES
TEST MODE
NO
INITIAL WAKEUP?
YES
CLEAR PREVIOUS STATUS FILE, SET INITIAL WAKEUP FILE, INITIALIZE PSEUDORANDOM REGISTER
NO
EEPROM ON; READ PREAMBLE, SYSTEM ID, TRANSMITTER ID, INVERTED DATA FLAG; EEPROM OFF
INPUT CURRENT STATUS, DETERMINE PRIORITY, SET COUNTER
PSEUDORANDON DELAY 0 TO 300ms
TRANSMITTER ON
TRANSMIT PREAMBLE, SYSTEM ID, TRANSMITTER ID, AND 3 STATUS BITS, CONCURRENTLY COMPUTING CRC
INPUT AND TRANSMIT BATTERY STATUS AND COMPLETE CRC
TRANSMIT CRC AND EOT
TRANSMITTER OFF
MORE TRANSMISSIONS?
YES
DELAY 100ms OR 850ms
NO
RESET TIMER
STANDBY ON
WAIT UNTIL ASLEEP

FIG. 4

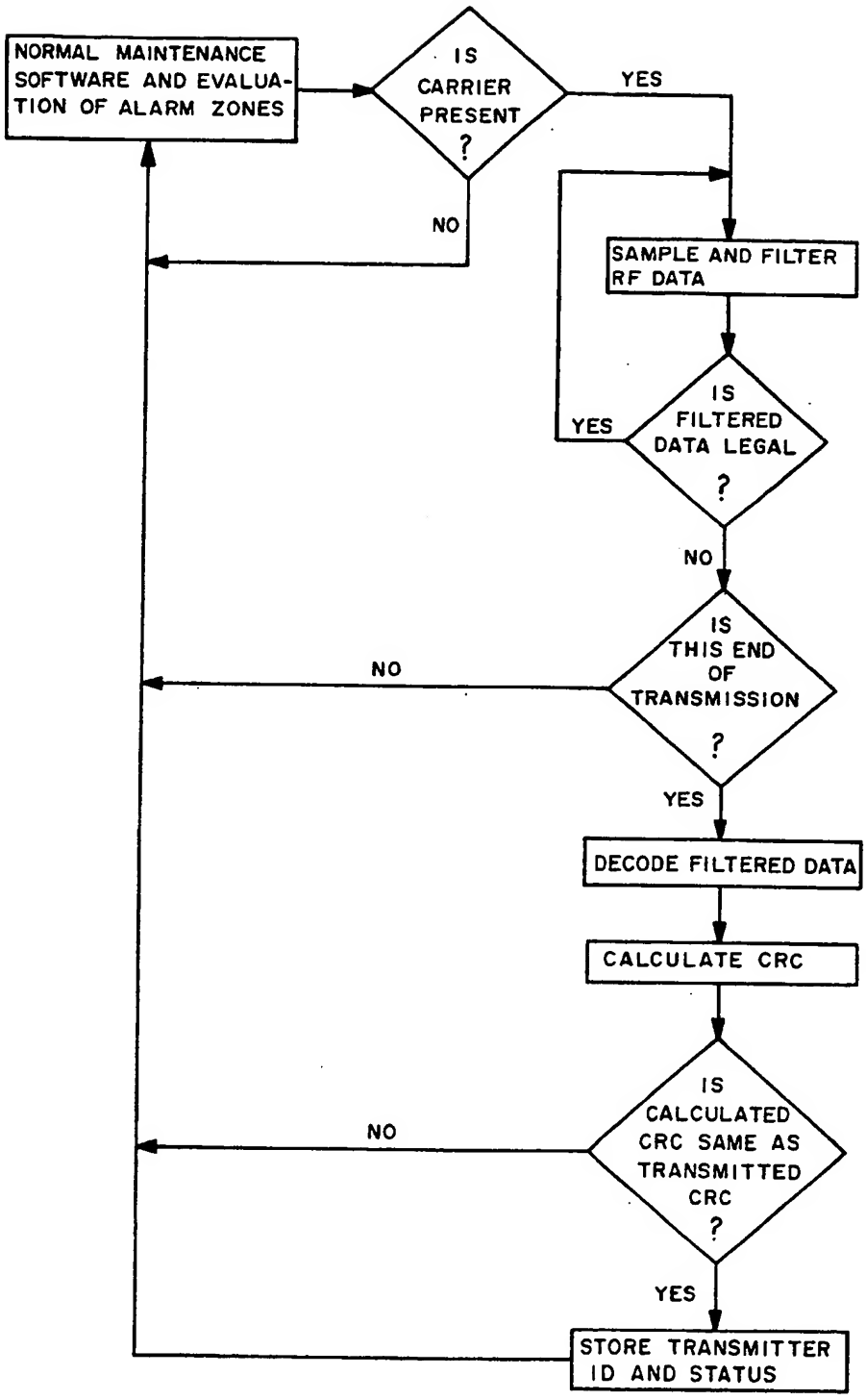
NORMAL MAINTENANCE SOFTWARE AND EVALUATION OF ALARM ZONES
IS CARRIER PRESENT ?
YES
NO
SAMPLE AND FILTER RF DATA
IS FILTERED DATA LEGAL ?
YES
NO
IS THIS END OF TRANSMISSION ?
NO
YES
DECODE FILTERED DATA
CALCULATE CRC
IS CALCULATED CRC SAME AS TRANSMITTED CRC ?
NO
YES
STORE TRANSMITTER ID AND STATUS

FIG. 5

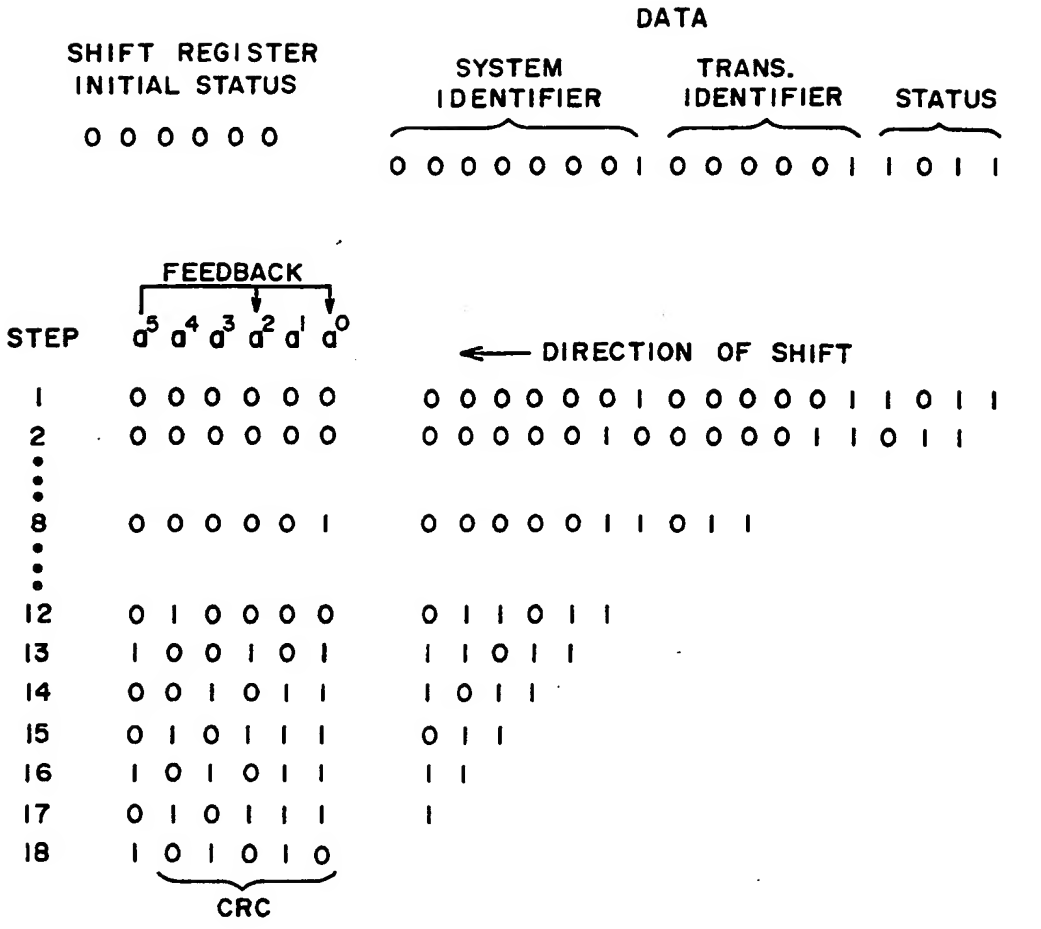
DATA
SHIFT REGISTER INITIAL STATUS
0 0 0 0 0 0
SYSTEM IDENTIFIER
TRANS. IDENTIFIER
STATUS
0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 1 1
FEEDBACK
STEP
a^5 a^4 a^3 a^2 a^1 a^0
DIRECTION OF SHIFT
1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 1 1
2 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 1 1
8 0 0 0 0 0 1 0 0 0 0 0 1 1 0 1 1
12 0 1 0 0 0 0 0 1 1 0 1 1
13 1 0 0 1 0 1 1 1 0 1 1
14 0 0 1 0 1 1 1 0 1 1
15 0 1 0 1 1 1 0 1 1
16 1 0 1 0 1 1 1 1
17 0 1 0 1 1 1 1
18 1 0 1 0 1 0
CRC
COMPLETE TRANSMISSION (DATA CRC)
0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 1 1 0 1 0 1 0

FIG. 6

SPECIFICATION

Security system with signal accuracy checking

The invention in general relates to security systems and in particular a wireless security system having one or more detector/sending units for reporting the existence of a condition of a central receiving unit.

Security systems which include one or more sending units which transmit coded radio frequency (r-f) signals to a central receiving unit which decodes the signals to produce an alarm or other indication of a condition at the sending unit location are well known. The condition may be the existence of a fire, an intrusion, an emergency, the presence of water or other fluid, or other condition desired to be monitored, or the condition may be the status of the sending unit, such as the condition of its battery or other sensor status. Generally, the information sent will also include the identity or location of the sending unit. A major problem with r-f or wireless security systems is the lack of reliability of the communicated data. The information or the condition, status, location etc. is generally transmitted serially as a string of digital data bits modulated on the r-f carrier wave which is received and demodulated by the central receiving unit to provide a digital data string to a processing circuit which analyses the data. Because of the nature of r-f communication, noise can disturb this process by causing unwanted transitions in otherwise valid transmitted data or by generating apparent data that is actually only noise. Since the processing circuitry analyses the received data for information about the status of the various sensors, noise in the data can cause a system to either reject a valid transmission or to falsely report an alarm status for one of the sensors. Previous attempts to solve this problem have involved transmitting the data several times and requiring the processing circuitry to receive multiple, identical data strings before reporting an alarm condition. This results in inefficient use of transmission time, leading to problems with battery life, clash (or collision) of transmissions from different sending units and meeting FCC regulations on net broadcast energy. This invention discloses a new approach for security systems to establish the accuracy and reliability of the received data.

It is one object of the invention to provide an improved security system, comprising transmitter means, that permits the communicated data signal to be reliably checked for accuracy.

The invention provides a security system comprising sensor means for sensing a condition at a location in a security area and producing a data signal representative of the condition at the location, means for producing an error check signal that is shorter than the data signal, transmitter means for transmitting an r-f signal modulated by the data signal and the error check signal, receiver means for receiving the modulated r-f signal, means utilising the received error check signal for checking the received data signal for accuracy and for selecting received signals that are accurate, and means responsive to the accurate data signal for producing an output indicative of the condition. Preferably the error check signal is a Cyclic Redundancy Check (CRC) code. Preferably the CRC code comprises the remainder when a polynomial representation of the data signal is divided by the polynomial $A^5 + A^2 + 1$. Preferably, the means for producing an error check signal comprises a microcomputer having a software-implemented shift register and the division is performed by shifting the data signal through the shift register while feeding back at least one bit into another bit.

The invention also provides a method of providing an indication of a condition at a protected location comprising the steps of: sensing the condition and providing a data signal representative of the condition, analysing the data signal to determine an error check signal that is shorter than the data signal, transmitting the data signal and error signal, receiving the transmitted signal, checking the received signal for accuracy, and utilising the accurate ones of the received signals to provide an indication of the condition at the protected location. Preferably the step of sensing and providing comprises providing a digital signal and the step of analysing comprises dividing the signal by a digital representation of an algebraic polynomial, and the step of transmitting includes transmitting the remainder left after the division (the CRC) along with the data signal. Preferably the step of checking comprises dividing the data portion of the received signal by the algebraic polynomial and comparing the remainder (the CRC) to the error check portion of the signal; i.e. the CRC calculated at the transmitter. In the preferred embodiment, there are eighteen bits of data and five bits of CRC code.

Use of an error check signal that is significantly shorter than the data signal, in systems and methods according to the invention, provides more reliable error checking than the repetition of the data signal and signal accuracy can be assured without the doubling or tripling of total transmission time that repetitive data transmissions require.

The invention further provides a detection system comprising a plurality of sending units, each of the units including a sensing means for sensing a condition, a means responsive to the sensing means for sending a data signal representative of the condition at randomised time intervals, and receiving means for receiving the data signals and producing an output indicative of the condition. Preferably the means for sending includes a means for generating a pseudo-random number, and a means for delaying the sending of the data signal for a time period related to the pseudo-random number. The sending of signals at a randomised time intervals markedly decreases the probability of synchronised clashing.

The invention also provides a method of providing an indication of a condition at a remote location comprising the steps of sensing the condition, waiting for a randomised time interval, sending a data signal representative of the condition, and receiving the data signal and utilising it to provide and indication of the condition. Preferably, the step of waiting comprises generating a pseudo-random number and waiting for a time interval related to the pseudo-random number. In the preferred embodiment, the step of

waiting for a time interval related to the pseudrandom number comprises cycling through a timing loop for a number of times equal to the pseudo-random number. The method may also include the step of waiting for an additional predetermined time interval.

According to algebraic coding theory, up to two errors in the received data will always result in a disagreement between the two calculated CRC's. In comparison, two transmissions of the same data signal can match if there are two errors; i.e. if the same bit in each transmission is erroneous. Thus, the apparatus and method of the invention provide better accuracy than the repetition of transmissions even though it would take eighteen bits to repeat a transmission as compared to the five bits the CRC requires in the preferred embodiment. Numerous other features, objects and advantages of the invention will become apparent from the following detailed description when read in conjunction with the accompanying drawings, of a detection system embodying the invention. It will be realised that this system has been selected for description to illustrate the invention by way of example.

In the accompanying drawings:-

Figure 1 is a schematic illustration of an exemplary detection system embodying the invention;

Figure 2 is an electrical circuit diagram of a portion of the sending unit of the illustrative system showing the electrical connections to the microcomputer,

Figure 3 is an electrical circuit diagram of the receiving unit of the system showing the connections to the microprocessor;

Figure 4 is a flow chart showing the steps of the microcomputer of the system;

Figure 5 is a flow chart showing the steps of the microprocessr program of the system; and

Figure 6 shows an example of the calculation of a CRC using a shift register.

Directing attention to Figure 1, a security system embodying the invention is shown. This embodiment includes three remote sending units 10, 11 and 12 and a central receiving unit 18. The sending units include an intrusion detector 10 on a door, a panic button unit 11, and fire detector unit 12, each of which produces a signal when the particular condition they are designed to detect occurs. Each remote detector unit 10, 11 and 12 has a radio frequency (r-f) transmitter 14, 15 and 16 respectively, associated with it which transmits a modulated r-f signal which includes a Cyclic Redundancy Check (CRC) code, which signal is received by the central unit 18. The central unit 18 demodulates the signals, calculates a second CRC and compres it to the transmitted CRC to determine if the transmitted signal is accurate, then decodes the accurate signals and provides outputs, such as flashing lights 20, a buzzer 21, or a signal 22 over a telephone line 23 to a supervising station (not shown), which indicate the conditions detected.

Turning now to a more detailed description of the detection system shown in Figure 1, the system includes an intrusion detector unit 10, a panic button 11 and a fire detector unit 12. It is understood that the three remote units shown are exemplary. An embodiment may have two such remote units or it may have hundreds. Other types of detectors than intrusion, panic and fire may also be included. For example, detectors which signal the presence of water where it should not be, or other unsafe or undesirable conditions may be included. Remote unit 10 includes a magnetic contact device 31 on a door which is connected via wire 32 to a signal processing circuit 33. The processing circuit 33 is connected to r-f transmitter 14 which transmits a signal to central unit 18 via antenna 34. Similarly, panic unit 11 comprises a panic button 35 which is connected to signal processing circuit 36, which is connected to transmitter 15, having antenna 37, and fire unit 12 comprises fire detector 38 which is connected to signal processor 39, which is connected to transmitter 16, having antenna 40. Central unit 18 includes antenna 42 which is connected to a receiver 88 (Figure 3) and signal processing circuitry within the chassis 43 of central unit 18. The signal processing circuitry is connected to annunciator lights 20, buzzer 21, and a telephone line 23. Other inputs and outputs shall be discussed in reference to Figure 3. It should be understood that the inputs and outputs are exemplary. In some embodiments, a variety of others may be used. It is also understood that a wide variety of other signals, such as battery status signals, supervision signals etc. may be transmitted between remote units 10, 11 and 12 and central unit 18.

A semi-block diagram of the circuitry of a processing circuit, such as 36 of an exemplary sending unit, such as 11, is shown in Figure 2, and a semi-block diagram of the circuitry of the central receiving unit 18 is shown in Figure 3. In these drawings, the numbers on the lines into the microcomputer 50 and the microprocessor 80, such as the "1" at the upper-left of the microcomputer 50, refer to the pin numbers of these two components. The labels within the microcomputer and microprocessor next to the pins, such as "OSC1" next to pin 1, refer to the internal signals of these computing units. The pin numbers and other details of the other components, such as EE Prom 51, transmitter 15, receiver 88, and memory 90 are not shown as details of such components are well known in the art.

The particular embodiment of the processing unit and transmitter shown in Figure 2 is a multipurpose one to which a number of different sensing devices, such as the panic button 35, fire detector 38, intrusion detector 31 or other devices may be connected. The interface (not shown) between the sensing devices such as 35, and the processing circuitry 36 is arranged so that the triggering of the device places a low signal on line 56 and on one of the input lines 57, 58 and 59. The details of the sensing devices 31, 35 and 38 as well as the interface will not be described in detail as these are well known in the art.

The processing circuit, such as 36, includes microcomputer 50, EE Prom 51, timer 53, inverter 54, ceramic resonator 62, resistors 63 through 66, capacitor 68 and diodes 70, 71, and 72. The processing circuit 36 also includes a power supply (not shown) which provides the voltage source required to use the circuitry, such as Vdd (75) and the ground, such as 76. Finally, the processing circuit 36 also includes a battery status circuit (not shown) which provides a low

signal on line 60 when the battery charge drops below a certain level. The power supply and battery status circuits are known in the art.

The number 1 pin of microcomputer 50 is connected to ground through ceramic resonator 62 and to the Vdd voltage through resistor 63. The number 2 pin is connected to the Vdd voltage. The number 3 pin is connected to the number 26 pin. The number 28 pin is connected to the output of inverter 54 through resistor 64. The input inverter 54 is connected to input line 56. The number 28 pin is also connected to the number 27 pin through resistor 65 and diode 70 in parallel, with the cathode of the diode toward the number 28 pin. The number 27 pin is also connected to ground through capacitor 68. The number 6 through 9 pins are connected to inputs 57 through 60. The number 24 pin is connected to the output of timer 53. The output of timer 53 is also connected to the input of inverter 54 through diode 71, with the cathode of the diode toward the timer. The number 25 pin is connected to the data output of EE Prom 51. The number 4 and 5 pins are connected to the system ground. The number 16 pin of the microcomputer 50 is connected to the (MR) input of timer 53 and to ground through resistor 66. The number 14 pin is connected to the input of inverter 54 through diode 72 with the cathode of the diode toward the microcomputer. The number 13 pin is connected to the power on input of the transmitter 15 and the number 17 pin is connected to the data input of the transmitter. The number 15 pin is connected to the power on input to the EE Prom 51. Pins 10, 11 and 12 are connected to the data input, chip select, and clock inputs, respectively, of EE Prom 51.

Figure 3 shows various components associated with central unit 18 and their connections to microprocessor 80. These components include tape deck 81, interface 83, programming unit 85, interface 87, receiver 88, power supply 89, memory 90, parallel outputs 91, parallel inputs 92, serial outputs 93, remote function 94, oscillator 99, transistor 100, resistors 101 through 105 and capacitors 109 and 110. The number 2 and 3 pins of microprocessor 80 are connected to the programming inputs of the central unit 18. Programming unit 85 may be connected to the these pins through an interface 87 or alternatively tape deck 81 may be connected through its interface 83. These components, 85 and 87 or 81 and 83, generally are connected only during the programming of the unit 18. The number 40 pin of microprocessor 80 is connected to the Vcc system voltage source and to the data output of receiver 88 through resistor 101. The data output of receiver 88 is also connected to pin 4 of the microprocessor. Pin 12 is connected to the carrier detect output of receiver 88 and to the Vcc voltage through resistor 102. The number 9 pin is connected to the drain of transistor 100 and to the Vcc voltage through resistor 103. The source of transistor 100 is connected to ground and the gate is connected to the reset output of the power supply 89. The power supply 89 provides the Vcc voltage 114 and a ground 115 for the system. The number 13 pin is connected to the Vcc voltage through resistor 104. The number 18 pin of microprocessor 80 is connected to the number 19 pin through oscillator 99 and to ground through capacitor 109. The number 19 pin is also connected to ground through capacitor 110. The number 20 pin is grounded and the number 31 pin is connected to ground through resistor 105. The number 6, 10, 11, 14 and 15 pins are connected to various remote functions, such as a modem, dialer etc. These functions include the telephone line 23 (Figure 1). Pins 1, 7 and 8 are connected to the serial outputs which may may include relays and other devices. The number 5 pin is connected to the reset input of the smoke detector auxiliary power circuit. The number 32-39 pins provide the parallel input/output function and are connected to both the parallel outputs, such as relays, LED's 20 and buzzer 21 and to the parallel inputs, which may include hardwired inputs to various sensors (providing a hardwire option for the system) and to various status inputs such as the battery and the memory unit. The number 16, 17 and 21-30 pins are connected to the central memory unit 90.

In the illustrative system, the parts of the circuits of Figures 2 and 3 are as follows: microcomputer 50 is a PIC 16C58, EE Prom 51 includes either an ER59256 or NMC9306N chip plus the FET and related circuitry to power the chip. Transmitter 15 may be one of many such transmitters known in the art plus associated buffers, transistors, etc. to turn on and off the transmitter and to shape the data prior to transmitting it. Timer 53 includes a 4541 programmable timer and its associated components, inverter 54 is one of a Schmitt trigger hex inverter package type 40106, resonator 62 is a 2M hertz ceramic resonator, resistors 63, 64, 65 and 66 are 2.2M ohm, 4.7K ohm, 82K ohm and 100K ohm respectively, capacitor 68 is 0.1M farad, and diodes 70, 71 and 72 are type 1N4148. Microprocessor 80 is preferably an Intel 8031 microcontroller, tape deck 81 and interface 83 may be a cassette deck or any other type of tape deck with an appropriate interface to match it with the microprocessor, programming unit 85 and interface 87 may be any mini, personal, or other type computer, with appropriate interfacing, receiver 88 may be one of many such receivers in the art, while the power supply, memory, parallel outputs and inputs, serial outputs and remote functions are all devices which are well known in the art. Preferably resistors 101, 102 and 104 are 10K ohm, while 103 and 105 are 4.7K and 1K ohm respectively, capacitors 109 and 110 are 30 picofarads, oscillator 99 is an 8 megahertz crystal oscillator, and transistor 100 is a type VN10KM.

Figure 4 shows a flow chart of the microcomputer 50 program of the system. Figure 5 shows a flow chart of the microprocessor 80 program of the system. Following the flow charts and referring to Figures 2, 3 and 6, the system functions as follows. To conserve battery power, microcomputer 50 is normally held in stand-by by a low signal on pin 28. The timer 53, however, operates continuously as long as a battery with sufficient charge is connected to the system. The timer 53 is programmed to change its output (the line connected to the cathode of diode 71) from high to low at appropriate times to make a supervisory report. This low signal is applied to the put of inverter 54 which causes its output to go high, placing a high signal on pin 28 of the micro-

computer 50 to turn it on. Or, a low signal from any one of the sensing devices (such as 31, 35, or 38) connected to input 56 will also place a high signal on microcomputer input pin 28 to turn it on. A short time after pin 28 goes high, pin 27 also goes high (with a delay determined by a resistor 65 and capacitor 68) and clears the microcomputer. Once turned on, the microcomputer drives its number 14 pin low to keep itself on. It then initialises the software, turns on the EE Prom 51 by placing a high signal on pin 15, enables the EE Prom by placing a high signal on pin 11 (chip select), reads the sending unit identification data from the EE Prom on pin 25 while clocking the EE Prom with a signal output on pin 12 and sending the address from which the data is to be read via pin 10.

The identification data consists of a preamble, system identification number, and transmitter identification number. The microcomputer 50 adds the current status (as defined by the inputs 6 through 8) to the identification data to provide a data signal to be transmitted. The microcomputer 50 then computers a 4-bit pseud-random number (0 through 15) as follows: a 15-bit shift register is initialised with a non-zero value. The contents of the register are shifted left, with the right-most bit (bit 1) replaced by the exclusive-OR of bits 14 and 15 (the two left-most bits). This new number in the register is the pseudo-random number which is used to determine the number of 20 millisecond delay loops to be executed by the microcomputer. This randomised delay may be from 0 to 300 milliseconds (15 × 20 milliseconds) and will average 150 milliseconds. Each successive shift of the 15-bit register will generate a new 15-bit number in a pseudo-random sequence. The sequence repeats after 32,767 numbers have been generated. Only 4-bits from the 15-bit number are used to determine the randomised delay.

The microcomputer 50 waits through the number of loop time periods determined by the pseudo-random number, then applies a high signal on pin 13. This high signal turns on the transmitter 15 and battery level indicator circuit (not shown). The preamble, system identification number, transmitter identification number and status are then output on pin 17. The battery status is then read on line 9 (a low signal indicates a low battery) and transmitted while a Cyclic Redundancy Check (CRC) is calculated as follows: If the data is A8,. . ., A1, T6,. . ., T1, S4,. . ., S1, where A1 through A8 represent the 8-bit system identifier code, T1 through T6 represent the 6-bit transmitter code, and S1 through S4 represent the 4-bit sensor status code, then using algebraic coding theory, the data plus the CRC can be interpreted as an algebraic polynomial, namely $A8\,a^{22} + A7\,a^{21} \ldots + S1a^5 + C5a^4 + C4a^3 + C3a^2 + C2a + C1$, where C5 through C1 is a 5-bit CRC. Algebraic coding theory states that the CRC should be chosen so that the above polynomial which we shall refer to as the "first polynomial" is exactly divisible by a second polynomial. In the preferred embdiment, the second polynomial is chosen as $a^5 + a^2 + 1$. The CEC may be determined by dividing the first polynomial with the CRC set to zero (C1 through C5 set to zero) by the second polynomial, and the remainder will then be the CRC. The division process is preferably performed in microcomputer 50 by a software-implemented shift register with feedback. In the preferred embodiment, a 6-bit shift register is implemented with feedback from the 6th-bit added without carry to bits one and three. The division, i.e. the progress of the data through the shift register is shown in Figure 6 for the sample data signal 0000000100000011011. Note that until step 13, no 1's are shifted into a^5, so until the data is shifted across the register with no change. In step 13 the 1 in a^5 is added without carry to a^2 and a^0. The shifting is continued through step 18, at which point the CRC is the lower order 5-bits of the shift register. The calculated CRC and an end of transmission signal (EOT) are then transmitted and the transmitter is turned off. After a supervisory transmission (activated by timer 53), the microcomputer then resets the timer by a high signal on pin 16 and returns itself to stand-by. Non-supervisory transmissions, however, are repeated with a predetermined fixed delay plus a pseudo-random delay before the microcomputer resets the timer and returns to stand-by. If the condition to be reported is on pins 6 or 7, the transmission is repeated nine times with a 100 millisecond predetermined fixed delay plus the random delay. If the condition to be reported is on input 8 (the panic button input), the transmitter is usually a portable unit. Because the transmitter's location is not fixed, signal strength may be marginal, so the transmission is repeated thirty times with an 850 millisecond fixed delay plus the random delay. In the preferred embodiment, the transmitted data word lasts 18 milliseconds. Supervisory transmission reporting is set to about 60 seconds by programming timer 53.

The transmitted signal is received by receiver 88 via antenna 42. Upon reception of a signal, the receiver puts a low signal on its carrier detect output which is applied to pin 12 of microprocessor 80 to turn the microprocessor on. Note that the preamble of the transmitted signal initiates the turn on process so that by the time the data arrives the microprocessor 80 is ready to receive it. The microprocessor 80 calculates a CRC, using the received data signal in the same manner as described above. The resulting remainder, or second CRC is subtracted from the received CRC and if they are the same the result will be zero and the received signal is gated to the outputs. If the result is non-zero the received signal is not passed to the output.

The preferred embodiments of the computer programs which calculate the pseudo-random number and the CRC in the transmitter and which calculate and check the CRC in the receiver are given at the end of the description of the system, just before the claims. Note that in the transmitter program the calculations are performed concurrently in the midst of other operations.

According to algebraic coding theory, up to two errors in the received data will always be signalled by a mismatch between the CRC received and the one calculated in the control unit 18. Thus, all single and double errors will be deleted. Further, most triple and quadruple errors will also be detected. Thus, the 5-digit CRC is more effective in catching

errors than the repeat transmission of the entire data signal, which in this case would require 18-bits of transmission.

A novel security system apparatus and method which provides for reliable accuracy checking of the transmitted data signal has been described. It is evident that those skilled in the art may now make many different embodiments and applications of the system without departing from the inventive concepts. For example, different polynomials may be used to calculate the error check code, or different software programming may be employed. Or the calculation may be performed using hardware or hard-wired circuits rather than software. Equivalent electronic parts and components may be used. Accordingly, the present invention is to be construed as embracing each and every novel feature and novel combination of features present in the detection system described without limitation by the particular embodiment used to illustrate the invention.

CLAIMS

1. A security system comprising:
sensor means for sensing a condition at a location in a security area and producing a data signal representative of the condition at the location;
means for producing an error check signal that is shorter than said data signal;
transmitter means for transmitting an r-f signal modulated by said data signal and said error check signal;
receiver means for receiving said modulated r-f signal;
means utilising said receiver error check signal for checking said received data signal for accuracy and for selecting received signals that are accurate; and
means responsive to said accurate signals for producing an output indicative of said condition.

2. A security system as in claim 1 wherein said error check signal comprises a signal representative of an algebraic code.

3. A security system as in claim 2 wherein said algebraic code comprises a cyclic code.

4. A security system as in any one of claims 1 to 3 wherein said data signal may be represented by a first polynomial and said error detection signal comprises the remainder when said first polynomial is divided by a second polynomial.

5. A security system as in claim 4 wherein said second polynomial is $a^5 + a^2 + 1$.

6. A security system as in claim 1 wherein said data signal and said error detection signal are digital signals and the number of bits of said error detection signal is less than the number of bits of said data signal.

7. A security system as in claim 6 wherein said error detection signal comprises a digital representation of an algebraic polynomial.

8. A security system as in claim 7 wherein said error detection signal comprises the remainder when said data signal is divided by an algebraic polynomial.

9. A security system as in claim 8 wherein said means for checking the accuracy of said received signal comprises a means for dividing said data signal by said algebraic polynomial and for comparing the result with said error detection signal.

10. A security system as in claim 9 wherein said algebraic polynomial is $a^5 + a^2 + 1$.

11. A wireless security system as in claim 6 wherein said means for producing an error check signal comprises a feedback shift register.

12. A security system as in claim 11 wherein said means for producing further comprises a computer and said feedback shift register is a software-implemented shift register.

13. A security system as in claim 6 wherein said means for checking comprises a feedback shift register.

14. A security system as in claim 13 wherein said means for checking further comprises a computer and said feedback shift register is a software-implemented shift register.

15. A method of providing an indication of a condition at a location protected by a security system comprising the steps of:
sensing said condition and providing a data signal representative of the condition;
analysing said data signal to determine an error check signal that is shorter than said data signal;
transmitting said data signal and said error signal;
receiving said transmitted signal;
checking said received signal for accuracy; and
utilising the accurate ones of said received signals to provide an indication of said condition.

16. The method of claim 15 wherein said step of sensing and providing a data signal comprises providing a digital signal, said step of analysing comprises dividing said signal by a digital representation of an algebraic polynomial, and said step of transmitting includes transmitting the remainder left after said division.

17. The method of claim 16 wherein said step of checking comprises dividing the data portion of said received signal by said algebraic polynomial and comparing the remainder of said error check portion of said received signal.

18. The method of claim 16 wherein said step of dividing comprises shifting said digital data signal through a shift register while feeding back at least one bit into at least one other bit.

19. The method of claim 18 wherein said step of shifting comprises shifting said data signal through a six-bit shift register in the direction of bit one to bit six, and said step of feeding back comprises adding the sixth bit without carry to bits one and three.

20. A detection system comprising:
a plurality of sending units, each of said units comprising: sensing means for sensing a condition, and means responsive to said sensing means for sending a data signal representative of said condition at randomised time intervals; and
receiving means for receiving said data signals and producing an output indicative of said condition.

21. The detection system of claim 20 wherein said means for sending includes:
a means for generating a pseudo-random number; and
a means for delaying the sending of said data

signal for a time interval related to said pseudo-random number.

22. The detection system of claim 21 wherein said means for generating a pseudo-random number includes a shift register.

23. The detection system of claim 21 wherein said means for delaying comprises a means for cycling through a number of time periods equal to said pseudo-random number.

24. The detection system of claim 21 and further comprising a means for delaying for a predetermined time interval in addition to said pseudo-random time interval.

25. A method of providing an indication of a condition at a remote location comprising:

sensing said condition;

waiting for a randomised time interval;

sending a data signal representative of said condition; and

receiving said data signal and utilising it to provide an indication of said condition.

26. The method of claim 25 wherein said step of waiting comprises generating a pseudo-random number and waiting for a time interval related to said pseudo-random number.

27. The method of claim 26 wherein said step of generating comprises placing a non-zero number in a shift register, and shifting the register contents while replacing one or more bits with the exclusive-OR of at least two other bits.

28. The method of claim 26 wherein said step of waiting comprises cycling through a timing loop a number of times equal to said pseudo-random number.

29. The method of claim 25 and further including the step of waiting for a predetermined time interval in addition to said randomised time interval prior to sending said data signal.

30. A security system constructed arranged and adapted to operate substantially as hereinbefore described with reference to the accompanying drawings.

31. A method of providing an indication of a condition substantially as hereinbefore described with reference to the accompanying drawings.

Printed for Her Majesty's Stationery Office by
Croydon Printing Company (UK) Ltd, 6/87, D8991685.
Published by The Patent Office, 25 Southampton Buildings, London, WC2A 1AY,
from which copies may be obtained.